

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-196616
(P2000-196616A)

(43)公開日 平成12年7月14日 (2000.7.14)

(51)Int.Cl. ¹	識別記号	F I	テマコード(参考)
H 04 L 12/28		H 04 L 11/20	D 5 J 1 0 4
9/08		H 04 Q 3/00	5 K 0 3 0
9/12		H 04 L 9/00	6 0 1 B 9 A 0 0 1
12/22			6 3 1
H 04 Q 3/00			11/26

審査請求 未請求 請求項の数21 O.L (全 17 頁)

(21)出願番号 特願平10-372206

(22)出願日 平成10年12月28日 (1998.12.28)

(71)出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者 小林 浩
東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内
(72)発明者 大和 克己
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(74)代理人 100083161
弁理士 外川 英明

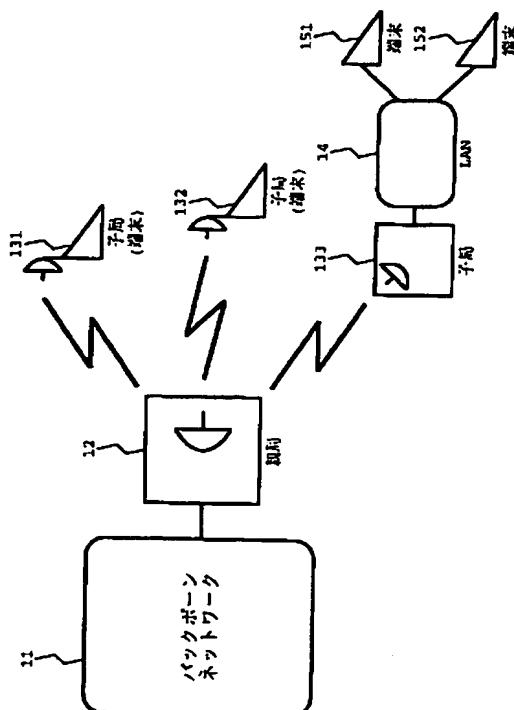
最終頁に続く

(54)【発明の名称】 情報通信ネットワークを用いた暗号化方式

(57)【要約】 (修正有)

【課題】ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザが攻撃から通信データを守る。

【解決手段】複数の子局131～133と、複数の子局と伝送媒体を用いてATMセルの送受信を行う親局12と、子局の一つと親局との組に対して与えられる、ATMセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、子局と親局との間での、セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新事項もしくは更新した暗号鍵を使用した事項を通知するセル暗号化鍵更新通知手段とを具備する。



【特許請求の範囲】

【請求項1】 バックボーンネットワークに接続する親局と複数の子局とを接続するアクセス回線に相当する共用の伝送媒体を備えた情報通信ネットワークにおいて、前記複数の子局と、前記複数の子局と前記伝送媒体を用いてATMセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ATMセルの送信時もしくは受信時に行う暗号化処理及び復号処理に用いるセル暗号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新事項もしくは更新した暗号鍵を使用した事項を通知するセル暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項2】 前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする、請求項1記載の情報通信ネットワークを用いた暗号化方式。

【請求項3】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、GFCフィールド内に割り当てられることを特徴とする請求項2記載の情報通信ネットワークを用いた暗号化方式。

【請求項4】 前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新事項もしくは更新したセル暗号化鍵を使用した事項を示すOAMセルを生成し送信することにより通知することを特徴とする、請求項1記載の情報通信ネットワークを用いた暗号化方式。

【請求項5】 前記子局の一つと前記親局との組に対して与えられる、セル暗号化鍵の送信時もしくは受信時に行う暗号化処理及び復号処理に用いる鍵暗号化鍵と、前記子局と前記親局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新事項もしくは更新した鍵暗号化鍵を使用した事項を通知する鍵暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項6】 前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする請求項5記載の情報通信ネットワークを用いた暗号化方式。

【請求項7】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、GFCフィールド内に割り当てられることを特徴とする請求項6記載の情報通信ネットワーク

を用いた暗号化方式。

【請求項8】 前記セル暗号化鍵更新通知手段および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新事項あるいは鍵暗号化鍵の更新事項もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵の使用事項を示すOAMセルを生成し送信することにより通知することを特徴とする請求項5記載の情報通信ネットワークを用いた暗号化方式。

【請求項9】 ネットワーク内の2ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でATMセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ATMセル送信時もしくは受信時に行う暗号化処理および復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間において、前記セル暗号化鍵の更新に伴ない同期を取るにあたって、ATMセルの送信側よりATMセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った事項もしくは更新した事項を通知するセル暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項10】 前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする請求項9記載の情報通信ネットワークを用いた暗号化方式。

【請求項11】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、VPIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VPIを規定のVPIフィールド長より短いフィールド長にて表すことを特徴とする請求項10記載の情報通信ネットワークを用いた暗号化方式。

【請求項12】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、VCIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、前記VCIを規定のVCIフィールド長より短いフィールド長にて表すことを特徴とする請求項10記載の情報通信ネットワークを用いた暗号化方式。

【請求項13】 前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵を更新した事項もしくは更新したセル暗号化鍵を使用した事項を示すOAMセルを生成し送信することにより通知することを特徴とする請求項9記載の情報通信ネットワークを用いた暗号化方式。

【請求項14】 前記第一のノード局と前記第二のノード局の組に対して与えられる、セル暗号化鍵の送信時もしくは受信時に行う暗号化処理、復号処理に用いる鍵暗号化鍵と、前記第一のノード局と前記第二のノード局と

の間での、前記鍵暗号化鍵の更新に伴う同期を取るため、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った事項もしくは更新した鍵暗号鍵を使用した事項を通知する鍵暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項15】 前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対しても変更することにより通知することを特徴とする請求項14記載の情報通信ネットワークを用いた暗号化方式。

【請求項16】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、VPIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VPIを規定のVPIフィールド長より短いフィールド長にて表すことを特徴とする請求項15記載の情報通信ネットワークを用いた暗号化方式。

【請求項17】 前記ATMセルヘッダ内の特定の少なくとも1ビットは、VCIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VCIを規定のVCIフィールド長より短いフィールド長にて表すことを特徴とする請求項15記載の情報通信ネットワークを用いた暗号化方式。

【請求項18】 前記セル暗号化鍵更新通知手段および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した事項もしくは更新したセル暗号化鍵あるいは鍵暗号鍵を使用した事項を示すOAMセルを生成し送信することにより通知することを特徴とする、請求項14記載の情報通信ネットワークを用いた暗号化方式。

【請求項19】 ATMセルを用いて通信を行うATMネットワークにおいて、ATMセルの送信時に、前記ATMセルのヘッダを圧縮するセルヘッダ圧縮手段と、前記セル圧縮手段により圧縮された前記ATMセルのヘッダ内の空き領域に、前記ATMセルに関わる制御情報を記載する制御情報記載手段と、ATMセルの受信時に前記制御情報記載手段により記載された前記ATMセルのヘッダ内の前記制御情報を除去する制御情報除去手段と、前記制御情報除去手段により除去された前記ATMセルのヘッダを規定の形に戻るように伸張するセルヘッダ伸張手段とを具備したことを特徴とするATMネットワーク。

【請求項20】 前記セルヘッダ圧縮手段は、VPIを規定のVPIフィールド長より短いフィールド長にて表すことを特徴とし、また前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じたVPIが記載されるフィールドの内に前記制御情報を記載することを特徴とする請求項19記載の情報通信ネットワーク

を用いた暗号化方式。

【請求項21】 前記セルヘッダ圧縮手段は、VCIを規定のVCIフィールド長より短いフィールド長にて表すことを特徴とし、また前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じたVCIが記載されるフィールドの内に前記制御情報を記載することを特徴とする請求項19記載の情報通信ネットワークを用いた暗号化方式。

【発明の詳細な説明】

10 【0001】

【発明の属する技術分野】 本発明は、例えば加入者無線アクセスシステムのように、交換やルーティングを司ったり、複数の子局に対するアクセス制御などを行う親局と、加入者装置などの子局とを接続するアクセス回線に相当する伝送媒体を、多数の子局にて共用し合うような、シェアードメディア型アクセスネットワークや、特定の2ノード局間の通信を提供するポイントツーポイント型ネットワーク、そして（「ATMセル」という。）を用いて通信を行うATMネットワーク等の情報通信ネットワークを用いた暗号化方式に関する。

【0002】

【従来の技術】 加入者無線アクセスシステム、（以下FTTH（Fiber To The Home）という。）、（以下HFC（Hybrid Fiber and Coaxial）という。）等のように、交換やルーティングを司ったり、子局に対するアクセス制御などを行う親局と、加入者装置などの子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合う、シェアードメディア型アクセスネットワークが、出現している。その中でも、アクセス回線を無線回線を用いて実現する加入者無線アクセスシステムは、アクセス回線を光ファイバやメタルケーブルを用いて実現しようとする場合アクセス回線の設置、取り換え及び保守を行う際に伴う、道路掘り起こし作業や電信柱に登っての作業が必要であった。他方、上述したシェアードメディア型アクセスネットワークでは、伝送媒体を多数の子局にて共有する、ポイントツーマルチポイント通信（以下「PTMP通信」という。）を提供するため、従来の電話網のように、交換局と加入者装置との間の伝送路をポイントツーポイント通信（以下「PTP通信」という。）にて提供する場合に比べて、セキュリティ上の脆弱さが問題となる。例えば、子局を改造することで、他の子局宛への通信データの盗聴が可能となる。そのため、シェアードメディア型アクセスネットワークでは、セキュリティ機能の強化が特に必要となる。

なお、無線ローカルループ（以下「WLL」という。）ネットワークのようにネットワーク事業者内のノード局間を無線回線にてポイントツーポイント通信を行うネットワークにおいても、伝送媒体に無線回線を使用しているという特徴上、セキュリティ機能の強化が同様に必要となる。

5

【0003】セキュリティ機能を強化するため、アプリケーション層においては、送信相手以外にメッセージ内容を読まれないように、送信メッセージに暗号化処理を施す機能、電子マネー等の情報をやりとりする場合に、偽造されたものではないことを確認できるよう、外部認証局が発行するデジタル署名によって差出人の身元を確認する機能等を搭載することが考えられる。

【0004】

【発明が解決しようとする課題】前出のように、アプリケーション層において暗号化処理機能やデジタル署名による身元確認機能を搭載することでセキュリティを強化する方法では、ユーザが意識してセキュリティ機能を起動することが前提となるため、ユーザにおいて機密情報を暗号化せずに送信してしまった場合には、通信データに対するセキュリティの保証が全くなされない。本発明の目的は上記の問題点に鑑み、親局と子局との間での伝送媒体（シェアードメディア）を介したPTMP通信を提供する上でのセキュリティ機能、さらには特定の2ノード局間のPTP通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ATMセルの転送を行うATM層においても提供するような、シェアードメディア型アクセスネットワーク、そしてポイントツーポイント型ネットワークを提供することにある。ところで、ATM層でのセキュリティ機能を提供するために、ATMセルのペイロード情報に対して暗号化処理を施す場合、さらなるセキュリティ強化のために、当該暗号化に用いる暗号化鍵を更新することが考えられる。その際に、ATMセルの送信側と受信側との間に、暗号化鍵の更新の同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いた暗号化鍵の更新を行った旨の情報、もしくは更新した暗号鍵を使用している旨の情報を通知する必要がある。しかしながら、ATM通信の標準化団体にて規定されたATMセルヘッダ内には、前記情報を記載するための領域が存在しない。

【0005】本発明の目的は上記の問題点も鑑み、暗号化鍵の更新の同期を取るために必要な情報をはじめとする、ATM通信の標準化団体にて規定されていない、ATMセルに関わる制御情報を記載するための領域を、ATMセルヘッダ内に確保することを可能とする、ATMネットワークを提供することにある。

【0006】

【課題を解決するための手段】上記目的を解決するために第一の発明は、親局と子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合うシェアードメディア型アクセスネットワークにおいて、複数の子局と、前記複数の子局と前記伝送媒体を用いてATMセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ATMセルの送信時、もしくは受信時に用いる暗号化処理、復号処理に用いるセル暗

6

号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新した暗号鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、を具備したことを特徴とする。なお、前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ATMセルヘッダ内の特定の少なくとも1ビットは、GFCフィールド内に割り当てられることを特徴とする。

【0007】また、前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵を使用している旨を示すOAMセルを生成し送信することにより通知することを特徴とする。このように構成することにより、親局と子局との間でのシェアードメディアを介したPTMP通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ATM層において、ATMセルに対して暗号化処理を施して当該ATMセルを送信するというセキュリティ機能を新たに提供することができ、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ATMセルの送信時の暗号化処理、復号処理の際に用いるセル暗号化鍵の更新に伴う、親局と子局との間で使用する鍵の更新の同期を、GFCフィールド値、もしくはOAMセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【0008】一方、第二の発明は、親局と子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合うシェアードメディア型アクセスネットワークにおいて、複数の子局と、前記複数の子局と前記伝送媒体を用いてATMセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ATMセルの送信時、もしくは受信時に用いる暗号化処理、復号処理に用いるセル暗号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新した暗号鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、前記子局の一つと前記親局との組に対して与えられる、セル暗号化鍵の送信時、もしくは受信時に用いる暗号化処理、復号処理に用いる鍵暗号化鍵と、前記子局と前記親局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送

信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った旨、もしくは更新した鍵暗号化鍵を使用している旨を通知する鍵暗号化鍵更新通知手段と、を具備したことを特徴とする。

【0009】なお、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ATMセルヘッダ内の特定の少なくとも1ビットは、GFCフィールド内に割り当てられることを特徴とする。また、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵を使用している旨を示すOAMセルを生成し送信することにより通知することを特徴とする。このように構成することにより、親局と子局との間でのシェアードメディアを介したPTMP通信を提供する上でのセキュリティ機能を、ATMセルの送信に対してだけでなく、ATMセルの暗号化処理、復号処理に用いるセル暗号化鍵の送信に対しても新たに提供することができる。さらに、親局と子局との間で使用する鍵の更新の同期を、セル暗号化鍵に対してだけでなく、鍵暗号化鍵に対しても、GFCフィールド値、もしくはOAMセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【0010】第三の発明は、ネットワーク内の2ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でATMセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ATMセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新したセル暗号化鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、を具備したことを特徴とする。なお、前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ATMセルヘッダ内の特定の少なくとも1ビットは、VPIが記載されるフィールド内に割り当てられ、前記第一のノード局と前記第二のノード局では、VPIを、規定のVPIフィールド長より短いフィ

ールド長にて表すことを特徴とする。

【0011】前記ATMセルヘッダ内の特定の少なくとも1ビットは、VCIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VCIを、規定のVCIフィールド長より短いフィールド長にて表すことを特徴とする。また、前記セル暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵を使用している旨を示すOAMセルを生成し送信することにより通知することを特徴とする。このように構成することにより、シェアードメディアを介したPTMP通信だけでなく、PTP通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ATM層において、ATMセルに対して暗号化処理を施して当該ATMセルを送信するというセキュリティ機能を新たに提供することができ、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ATMセルの送信時の暗号化処理、復号処理の際に用いるセル暗号化鍵の更新に伴う、ノード局間で使用する鍵の更新の同期を、VPIフィールドまたはVCIフィールドを圧縮することにより生じる空きビット領域、もしくはOAMセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【0012】一方、第四の発明は、ネットワーク内の2ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でATMセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ATMセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ATMセルの送信側よりATMのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新したセル暗号化鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、前記第一のノード局と前記第二のノード局の組に対して与えられる、セル暗号化鍵の送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った旨、もしくは更新した鍵暗号化鍵を使用している旨を通知する鍵暗号化鍵更新通知手段と、を具備したことを特徴とする。

【0013】なお、前記セル暗号化鍵更新通知手段、お

および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ATMセルヘッダ内の特定の少なくとも1ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対しても変更することにより通知することを特徴とする。前記ATMセルヘッダ内の特定の少なくとも1ビットは、VPIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VPIを、規定のVPIフィールド長より短いフィールド長にて表すことを特徴とする。前記ATMセルヘッダ内の特定の少なくとも1ビットは、VCIが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、VCIを、規定のVCIフィールド長より短いフィールド長にて表すことを特徴とする。また、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ATMセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵を使用している旨を示すOAMセルを生成し送信することにより通知することを特徴とする。

【0014】このように構成することにより、PTP通信を提供する上でのセキュリティ機能を、ATMセルの送信に対してだけでなく、ATMセルの暗号化処理、復号処理に用いるセル暗号化鍵の送信に対しても新たに提供することができる。さらに、ノード局間で使用する鍵の更新の同期を、セル暗号化鍵に対してだけでなく、鍵暗号化鍵に対しても、VPIフィールドまたはVCIフィールドを圧縮することにより生じる空きビット領域、もしくはOAMセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。第五の発明は、ATMセルを用いて通信を行うATMネットワークにおいて、ATMセルの送信時に、前記ATMセルのヘッダを圧縮するセルヘッダ圧縮手段と、前記セル圧縮手段により圧縮された前記ATMセルのヘッダ内の空き領域に、前記ATMセルに関わる制御情報を記載する制御情報記載手段と、ATMセルの受信時に、前記制御情報記載手段により記載された前記ATMセルのヘッダ内の前記制御情報を除去する制御情報除去手段と、前記制御情報除去手段により除去された前記ATMセルのヘッダを規定の形に戻るように伸張するセルヘッダ伸張手段と、を具備したことを特徴とする。

【0015】前記セルヘッダ圧縮手段は、VPIを規定のVPIフィールド長より短いフィールド長にて表すことを特徴とし、また、前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じた、VPIが記載されるフィールドの内に前記制御情報を記載することを特徴とする。前記セルヘッダ圧縮手段は、VCIを規定のVCIフィールド長より短いフィールド長にて

表すことを特徴とし、また、前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じた、VCIが記載されるフィールドの内に前記制御情報を記載することを特徴とする。このように構成することにより、暗号化鍵の更新の同期を取るために必要な情報をはじめとする、ATM通信の標準化団体にて規定されていない、ATMセルに関わる制御情報を記載するための領域を、VPIフィールド、VCIフィールドをはじめとするATMセルヘッダ内に確保することができる。

10 【0016】

【発明の実施の形態】図1は、この発明に係わるシェアードメディア型アクセスマッシュワークの一つである、加入者無線アクセスシステムのアーキテクチャの一実施の形態を示す図である。図1において、11はバックボーンネットワーク、12は交換やルーティングを司ったり、子局に対するアクセス制御などを行う親局、131～133は加入者装置などの子局である。親局12と子局131～133は伝送媒体として無線回線が用いられている。また、バックボーンネットワーク11と親局12とは、有線回線もしくは無線回線を用いて接続される。そして、子局133にはLAN14を介して端末151、152が接続されており、子局131、132は端末である。図1に示す加入者無線アクセスシステムでは、親局12と子局131～133との間の通信を無線回線という同一の伝送媒体を用いて行うため、親局とある子局との間の通信データを、他の子局が盗聴することは、自身の子局を改造することで容易に行うことができる。本発明では、このような他の子局による通信データの盗聴を防ぐためのセキュリティ機能を、従来アプリケーション層にて施されている、エンドツーエンドのセキュリティ機能とは別に提供する。

【0017】図2は、図1に示した加入者無線アクセスシステムがATM（非同期転送モード）を用いて通信を行う場合の、親局12と端末151（もしくは端末152）との間のプロトコルスタック（図2の（a））、そして親局12と子局131（もしくは子局132）との間のプロトコルスタック（図2の（b））を示す。図2において、Applic.はアプリケーション層を、AALはATMアダプテーション層を、ATMはATM層を、PHYは物理層を示す。また、WALは無線アクセス層を示し、無線回線上でATM通信を実現するためのプロトコルを規定している。本発明では、他の子局と共有する無線回線を使用した通信が行われる、親局と子局との間でのデータ通信に対してセキュリティ機能を新たに搭載する。そのために、親局、子局のATM層に、セキュリティ機能を搭載するものとする（ATM+Sec層）。ATM+Sec層では、通常のATM層にて行う動作に加えて、以下の動作を行うことが可能である。（1）受信したATMセルのペイロード情報を暗号化する。（2）受信したATMセルのペイロード情報が暗号化さ

11

れていれば、本情報を復号する。

【0018】このようにATMセルを単位に暗号化する場合、ATM層の上位層に混在する様々なサービス（IP（インターネットプロトコル）パケット転送サービス、MAC（メディアアクセス制御）パケット転送サービス、音声データサービス、専用線サービス、等）に対するセキュリティ機能の強化を、これらのサービスに依存せずに、ATM層にて統一した方法にて提供することが可能となる。図3～図5は、図2に示したATM+Sec層にて行う、暗号化、復号の手順を示す機能ブロック図である。図3の方法では、親局より子局宛への、下り方向のATMセルの送信を行う場合、親局内の暗号化部211において、親局が保持する子局用の公開鍵を用いてATMセルの暗号化処理を行い、子局内の復号化部221において、子局が保持する秘密鍵を用いて暗号化されたATMセルの復号処理を行う。また逆に、子局より親局宛への、上り方向のATMセルの送信を行う場合、子局内の暗号化部222において、子局が保持する親局用の公開鍵を用いてATMセルの暗号化処理を行い、親局内の復号化部212において、親局が保持する秘密鍵を用いて暗号化されたATMセルの復号処理を行う。図3の方法の場合、親局内の暗号化部211にて用いる公開鍵、復号化部212にて用いる秘密鍵、子局内の暗号化部222にて用いる公開鍵、復号化部221において用いる秘密鍵は、各々異なるものとなる。

【0019】図4の方法では、親局内の暗号化／復号化部21、子局内の暗号化／復号化部22において用いられる鍵は、親局内の鍵a生成部23にて生成される鍵aである。そして、親局より子局に対して鍵aを送信する際に、親局内の暗号化部24において、親局が保持する子局用の公開鍵を用いて鍵aの暗号化処理を行い、子局内の復号化部25において、子局が保持する秘密鍵を用いて暗号化された鍵aの復号処理を行う。なお、鍵aの送信には、例えばATM通信にて規定されるOAMセル(Operation Administration and Maintenanceセル)を用いることが考えられる。図4の方法の場合、鍵a生成部において鍵aの更新を定期的もしくはランダムな時間間隔に行うことと、送信中のATMセルの盗聴に対するより強固な防御が実現でき、図3の方法に比べて、さらなるセキュリティ機能の強化が実現できる。また一般に、暗号化処理、復号処理を同一な鍵aを用いて実行する共通鍵方式の方が、暗号化処理に用いる鍵（公開鍵）と復号処理に用いる鍵（秘密鍵）とを別個に用意する公開鍵方式よりも、暗号化／復号の処理速度が速いので、より高速な通信に向いている。

【0020】図5の方法では、親局内の暗号化／復号化部21、子局内の暗号化／復号化部22において用いられる鍵aを送信する際に、親局内にて暗号化処理を行う暗号化部24、子局内にて復号処理を行う復号化部25において用いられる鍵は、親局内の鍵b生成部26にて

12

生成される鍵bである。そして、親局より子局に対して鍵bを送信する際に、親局内の暗号化部27において、親局が保持する子局用の公開鍵を用いて鍵bの暗号化処理を行い、子局内の復号化部28において、子局が保持する秘密鍵を用いて暗号化された鍵bの復号処理を行う。なお、鍵bの送信には、例えばATM通信にて規定されるOAMセルを用いることが考えられる。図5の方法の場合、鍵a生成部における鍵aの更新を定期的もしくはランダムな時間間隔に行うと共に、鍵b生成部において鍵bの更新を定期的もしくはランダムな時間間隔に行うことで、親局より子局宛に送信される鍵aの盗聴に対するより強固な防御が実現でき、図4の方法に比べて、さらなるセキュリティ機能の強化が実現できる。例えば、鍵aの更新は半日程度毎に、鍵bの更新は一週間程度毎に更新する。なお、公開鍵、秘密鍵を用いた暗号化処理、復号処理（図3におけるATMセルの暗号化処理、復号処理、図4における鍵aの暗号化処理、復号処理、図5における鍵bの暗号化処理、復号処理）には、例えばRSA方式(Rivest Shamir Adleman方式)や楕円暗号方式などの公開鍵方式を用いて行い、鍵a、鍵bを用いた暗号化処理、復号処理（図4、5におけるATMセルの暗号化処理、復号処理、図5における鍵aの暗号化処理、復号処理）には、例えばDES方式(Data Encryption Standard方式)やFEAL方式(Fast Encryption Algorithm方式)などの共通鍵方式を用いて行う。現在のコンピュータ処理能力から、公開鍵方式では768ビット以上のビット長の鍵を、共通鍵方式では64ビット以上のビット長の鍵を用いるのが適当である。

【0021】本明細書では、セキュリティ機能が一番強固であると考えられる図5の方法を用いた場合の、本発明の実施の形態を、以降において説明する。図6、図7に、図5に示した機能ブロック図にて用いられる共通鍵a、bの更新の手順を示す。通常、暗号鍵は有効期限を有しており、同期限内に暗号鍵を更新しなければ無効となってしまうため、以降の送信データの復号が不可能となってしまう。図6に示した手順では、暗号鍵を生成する親局が、当該鍵の有効期限前の一定期間に入ると新たな鍵を生成して、子局宛に送信を行う。なお、子局の立ち上げ時に限り、子局より親局宛へ当該子局が立ち上がった旨を通知し、親局にて当該子局の認証を行い、その後に暗号鍵の生成、送信を行う。図7に示した手順では、子局が、暗号鍵の有効期限前の一定期間に入ると、新たな鍵を生成するよう親局宛に共通鍵の生成要求を送信する。なお、子局の立ち上げの際には、子局より親局宛へ当該子局が立ち上がった旨を通知すると共に暗号鍵の生成要求を送信し、親局にて当該子局の認証を行った後に、暗号鍵の生成、送信が行われるようにする。図6および図7に示した手順に従い、親局と子局とにおいて暗号鍵の更新を行う場合、更新前の暗号鍵と更新後の暗号鍵とのいずれの鍵により暗号化処理、復号処理を行う

かを確認する、換算すれば親局と子局との間で鍵更新の同期を取る必要がある。本発明では、暗号鍵の更新の同期を、(1) ATMセルヘッダ内の情報(GFCフィールドなど)を用いる方法(2) OAMセルを用いる方法のいずれかの方法にて実現する。

【0022】まず、ATMセルヘッダ内の情報を用いて暗号鍵の更新の同期を取る方法について説明する。図8に、親局と子局との間で伝送されるATMセルのフォーマットを示す。図1に示す加入者無線アクセスシステムでは、キャリアが提供するバックボーン網側の設備である親局と、ユーザ側の設備である子局とのインターフェースは、UNI(ユーザ網インターフェース)が用いられるので、図8に示したATMセルのフォーマットは、UNIにて定義されるものである。図8に示すように、ATMセルは、情報伝送に必要な情報を格納する5バイト長のヘッダ31と、伝達情報を格納する48バイト長のペイロード32から構成される。ヘッダ31内には、4ビット長のGFC(Generic Flow Control)フィールド33が存在する。ITU-Tの規格においては、GFCフィールドは、通信網と端末との間でローカルに行われるフロー制御のために設けたフィールドであるが、通常はGFCフィールドを用いたフロー制御を必要としない。そこで、本発明では、GFCフィールドのうち1ビットを、暗号鍵の更新の同期を取るために使用する。図9、図10に、GFCフィールドの1ビットを用いた暗号鍵の同期の手順を示す。なお、図9では、共通鍵の生成を行う親局より子局宛にATMセルを送信する場合を、図10では、子局より親局宛にATMセルを送信する場合を示す。

【0023】図9、図10共に、送信側では、ATMセルの暗号化に用いた暗号鍵を更新する度に、当該ATMセル内のGFCフィールドのあらかじめ定められた1ビット(図9、図10では、GFCフィールドの下位1ビット)を反転させて送信する。そして受信側では、受信したATMセルのGFCフィールドの前記1ビットが、前回受信したATMセルの1ビットと反転した値であれば、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたATMセルであることが分かるため、以後、GFCフィールドの前記1ビットが反転したATMセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。本方式により、受信側においては、送信側が暗号化処理に用いた暗号鍵が更新前の鍵であるか更新後の鍵であるかを陽に理解することができるため、暗号鍵の定期的あるいはランダムな時間周期で更新を伴う場合にも、復号処理を正確に行うことができる。また、暗号鍵の更新の同期を、未使用領域であるATMセルヘッダ領域内(GFCフィールド)の1ビットのみを用いて実現するため、スループットの低下をもたらすことはない。なお、ATMセルの暗号化を行う加入者無線アクセスシステム以外のネットワークノード(A

TM交換機、もしくは端末)において、GFCフィールド内の値に基づくフロー制御機能が搭載されている場合、上述したように暗号鍵の更新の同期を行うために設定したGFCフィールド値を前記ノードにそのまま引き渡すと、予期せぬ動作を引き起こしかねない。そのため、本発明を実施する場合には、暗号鍵による復号処理を終えた受信側では、GFCフィールドの値4ビットを全て「0」と設定するという手順を行うように規定し、加入者無線アクセスシステム以外のネットワークノードにおいても、GFCフィールドを用いたフロー制御は行われないようにするという手順を行ってもよい。また、暗号鍵の更新の同期を取るために、前述のようにGFCフィールド内の特定の1ビットを割り当てる他にも、VPI値、VCI値のいずれか、もしくは両値を圧縮して運用することで、VPIフィールド(8ビット長)もしくはVCIフィールド(16ビット長)のいずれか、もしくは両フィールドのうちの一部フィールドに空きビット領域を用意し、本領域を暗号鍵の更新の同期を取るために用いる方法が考えられる。なお、本方法については、別途説明する。

【0024】次に、OAMセルを用いて暗号鍵の更新の同期を取る方法について説明する。図11、図12に、OAMセルを用いた暗号鍵の同期の手順を示す。なお、図11では、共通鍵の生成を行う親局より子局宛にATMセルを送信する場合を、図12では、子局より親局宛にATMセルを送信する場合を示す。図11、図12共に、送信側では、ATMセルの暗号化に用いた暗号鍵を更新する度に、以後のATMセルに対しては新たな暗号鍵を用いて暗号化を行う旨を示すOAMセルを送信する。そして受信側では、OAMセルを受信することで、以後に到着するATMセルが、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたものであることが分かるため、以後、OAMセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。なお、図11に示すように、共通鍵の生成を行う親局がデータの送信側となる場合には、暗号鍵を送信するために用いるOAMセルのみを送信するだけで、受信側である子局においては、以後の親局から送信されるATMセルは、当該OAM内に挿入されている、更新後の暗号鍵を用いて暗号化されるものと認識するようにし、上記OAMセルとは別に、更新後の暗号鍵を用いて暗号化を開始した旨を示すOAMセルを送信する必要はない。ところで、暗号鍵を更新した旨をOAMセルにて通知する場合、廃棄等により受信側にて当該OAMセルが正しく受信できなければ、受信側では暗号鍵が更新された旨を知ることができず、以降に受信するATMセルの復号も更新前の暗号鍵を用いて試みるため、ATMセルの復号が正しく行われない。これを解決するため、例えば、受信側においては、暗号鍵を更新した旨を示すOAMセルを受信すれば、ACKを示すセル(OAMセルを用いて定

義)を折り返し送信側に送信し、送信側においては、当該ACKを示すセルの受信を待って、新たな暗号鍵に更新するという手段を用いることが考えられる。この場合、送信側では、暗号鍵を更新した旨を示すOAMセルを送信した後も、当該OAMセルに対するACKを示すセルを受信するまでは、引き続いて更新前の暗号鍵を用いてATMセルの暗号化を行い、また、一定時間が経過してもACKを示すセルが受信できなければ、送信側は再度暗号鍵を更新した旨を示すOAMセルを送信する。

【0025】他の方法としては、ACKを示すセルを用いて鍵の更新通知の確認を待つことなく、ATMセルを更新後の暗号鍵を用いて暗号化して送信し、受信側では正しく復号できたか否かを、例えばパリティチェック機能を用いて認識するという手段も考えられる。この場合、正しく復号できなかつたと判断した受信側では、その旨を送信側へ通知し、送信側において、再度暗号鍵を更新した旨を示すOAMセルの送信を行う。図13は、子局の電源投入時(立ち上げ時)に行われる、親局での当該子局の認証シーケンスを示す。子局では、電源投入時に、子局の認証要求として、公開鍵と子局の識別番号を親局に対して送信する。なお、子局には、当該子局の識別番号、公開鍵、秘密鍵が、予め(子局の製造時、出荷時、等に)記載されている。親局では、送られてきた子局の識別番号が登録されてるものと一致すれば、鍵暗号化鍵(図5における鍵b)を生成し、これを当該子局より送られてきた公開鍵を使って暗号化し、子局に返送する。子局では、子局内に格納している秘密鍵を使ってこれを復号し、鍵暗号化鍵を取得する。次に子局は、鍵暗号化鍵を使って、子局を利用するユーザが入力したパスワード(もしくはこれに代替し得るもの)を暗号化し、親局に送付する。親局では、同じ鍵暗号化鍵を使って復号し、登録されているパスワードと一致すれば正しい子局と認定し、認証手続きを終了する。

【0026】図14は、子局の機能ブロック図の一例である。ATMセル受信部401は、子局がLANもしくは端末と接続する場合は(図1に示す子局133)、接続されるノードより発せられるATMセルを受信し、子局が端末である場合は(図1に示す子局131、132)、子局の上位層にて生成されるATMセルを受信する。ATMセル受信部401にて受信したATMセルは、VPI/VCI識別部402に転送され、当該ATMセルが属するフロー(VPI/VCIにて一意に識別可能)に基づき、当該ATMセルの暗号化を行うか否かを判断する。暗号化を行わないフローである場合は、ATMセル送信部403を介して、親局宛に当該セルは送信され、暗号化を行うフローである場合は、当該セルをセル暗号化処理部404へ引き渡し、当該セルのペイロード部の暗号化を行う。セル暗号化処理部404に引き渡されたATMセルは、セル暗号化鍵記憶部405にて記憶されるセル暗号化鍵(図5に示す鍵a)を用いて暗

号化が行われた後に、ATMセル送信部403を介して、親局宛に送信される。このとき、GFCフィールドを用いて親局とのセル暗号化鍵の更新の同期を取る場合は、GFCビット設定部406により、セル暗号化鍵の更新が行われた際に、所定のビットの反転が行われるよう、GFCビット値の設定が行われる。また、OAMセルを用いて親局とのセル暗号化鍵の更新の同期を取る場合は、セル暗号化鍵の更新が行われた際に、鍵の更新を行った旨を示すOAMセルをOAMセル生成部407にて生成し、親局宛に送信する。なお、セル暗号化鍵の有効期限に伴う新たなセル暗号化鍵の生成要求を親局宛に行う場合は、その旨を示すOAMセルをOAMセル生成部407にて生成し、親局宛に送信する。

【0027】親局より送信されるATMセルを受信するATMセル受信部408では、受信したATMセルがOAMセルでなければ、当該セルをVPI/VCI識別部409に転送して、当該ATMセルが属するフローに基づき、当該ATMセルが暗号化されたATMセルであるか否かを判断する。暗号化されていないATMセルである場合は、ATMセル送信部410を介して、当該子局に接続されるノード宛、もしくは当該子局の上位層へATMセルを送信する。そして当該ATMセルが暗号化されたATMセルである場合は、当該セルをセル復号処理部411へ引き渡し、当該セルのペイロード部の復号を行う。セル復号処理部411に引き渡されたATMセルは、セル暗号化鍵記憶部405にて記憶されているセル暗号化鍵を用いて復号が行われた後に、ATMセル送信部410を介して、送信される。このとき、セル暗号化鍵更新検査部412において、セル復号処理部411に引き渡されたATMセル内のGFCビット値のチェック、もしくは、OAMセル処理部413にてセル暗号化鍵の更新を行った旨のOAMセルを受信したか否かのチェックを行い、セル復号処理部411にて使用するセル暗号化鍵を更新するか否かを、セル暗号化鍵記憶部405へ通知する。

【0028】OAMセル処理部413では、セル暗号化鍵の更新を行った旨を示すOAMセルの他に、セル暗号化鍵を含むOAMセル、そしてセル暗号化鍵の暗号化処理、復号処理に用いる鍵暗号化鍵(図5に示す鍵b)を含むOAMセルを受信する。暗号化されたセル暗号化鍵を含むOAMセルを受信した場合は、当該鍵をセル暗号化鍵復号処理部414へ引き渡し、鍵暗号化鍵記憶部415内の鍵暗号化鍵を用いて、セル暗号化鍵を復号し、セル暗号化鍵記憶部405へ引き渡す。また、暗号化された鍵暗号化鍵を含むOAMセルを受信した場合は、当該鍵を鍵暗号化鍵復号処理部416へ引き渡し、秘密鍵記憶部417内の秘密鍵を用いて、鍵暗号化鍵を復号し、鍵暗号化鍵記憶部415へ引き渡す。なお、鍵暗号化鍵の有効期限に伴う新たな鍵暗号化鍵の生成要求を親局宛に行う場合は、その旨を示すOAMセルをOAMセ

ル生成部507にて生成し、親局宛に送信する。図15は、親局の機能ブロック図の一例である。子局より送信されるATMセルを受信するATMセル受信部501では、受信したATMセルがOAMセルでなければ、当該セルをVPI/VCI識別部502に転送して、当該ATMセルが属するフロー(VPI/VCIにて一意に識別可能)に基づき、当該ATMセルが暗号化されたATMセルであるか否かを判断する。暗号化されていないATMセルである場合は、ATMセル送信部503を介して、当該親局が接続するバックボーン網宛へATMセルを送信する。そして当該ATMセルが暗号化されたATMセルである場合は、当該セルをセル復号処理部504へ引き渡し、当該セルのペイロード部の復号を行う。

【0029】セル復号処理部504に引き渡されたATMセルは、セル暗号化鍵記憶部505にて記憶されるセル暗号化鍵(図5に示す鍵a)を用いて復号が行われた後に、ATMセル送信部503を介して、送信される。このとき、セル暗号化鍵更新検査部506において、セル復号処理部504に引き渡されたATMセル内のGFCビット値のチェック、もしくは、OAMセル処理部507にてセル暗号化鍵の更新を行った旨のOAMセルを受信したか否かのチェックを行い、セル復号処理部504にて使用するセル暗号化鍵を更新するか否かを、セル暗号化鍵記憶部505へ通知する。バックボーン網より送信されるATMセルを受信するATMセル受信部508にて受信したATMセルは、VPI/VCI識別部509に転送され、当該ATMセルが属するフローに基づき、当該ATMセルの暗号化を行うか否かを判断する。暗号化を行わないフローである場合は、ATMセル送信部510を介して、子局宛に当該セルは送信され、暗号化を行うフローである場合は、当該セルをセル暗号化処理部511へ引き渡し、当該セルのペイロード部の暗号化を行う。セル暗号化処理部511に引き渡されたATMセルは、セル暗号化鍵記憶部505にて記憶されるセル暗号化鍵を用いて暗号化が行われた後に、ATMセル送信部510を介して、子局宛に送信される。このとき、GFCフィールドを用いて子局とのセル暗号化鍵の更新の同期を取る場合は、GFCビット設定部512により、セル暗号化鍵の更新が行われた際に、指定したビットの反転が行われるよう、GFCビット値の設定が行われる。また、OAMセルを用いて子局とのセル暗号化鍵の更新の同期を取る場合は、セル暗号化鍵の更新が行われた際に、鍵の更新を行った旨を示すOAMセルをOAMセル生成部513にて生成し、子局宛に送信する。

【0030】セル暗号化鍵生成部514では、セル暗号化鍵の有効期限に伴う新たなセル暗号化鍵の生成を、セル暗号化鍵記憶部505からの要求、もしくは子局からの要求(OAMセル処理部507にて認識した後に通知)により行う。セル暗号化鍵生成部にて生成されたセル暗号化鍵は、セル暗号化鍵記憶部505に引き渡すと

共に、セル暗号化鍵暗号化処理部515にて暗号化を行った後に、OAMセル生成部513にて当該鍵を挿入したOAMセルを生成し、これを子局宛に送信する。セル暗号化鍵暗号化処理部515では、鍵暗号化鍵記憶部516内に保持される鍵暗号化鍵(図5に示す鍵b)を用いて、セル暗号化鍵の暗号化を行う。鍵暗号化鍵生成部517では、鍵暗号化鍵の有効期限に伴う新たな鍵暗号化鍵の生成を、鍵暗号化鍵記憶部516からの要求、もしくは子局からの要求(OAMセル処理部507にて認識した後に通知)により行う。鍵暗号化鍵生成部にて生成された鍵暗号化鍵は、鍵暗号化鍵記憶部516に引き渡すと共に、鍵暗号化鍵暗号化処理部518にて暗号化を行った後に、OAMセル生成部513にて当該鍵を挿入したOAMセルを生成し、これを子局宛に送信する。鍵暗号化鍵暗号化処理部518では、公開鍵記憶部519内に保持される公開鍵を用いて、鍵暗号化鍵の暗号化を行う。

【0031】以上、本発明の実施の形態を加入者無線アクセスシステムを用いて説明したが、これらの発明の実施の形態は、加入者無線アクセスシステムに限らず、親局と複数の加入者との間にて行う通信を同一の伝送媒体を用いて行う、シェアードメディア型アクセネットワーク全てに適用できるものである。また、上記説明では、親局にてセル暗号鍵及び鍵暗号鍵を生成するとしているが、どちらか一方もしくは両者の機能を子局が具備しても同様のセキュリティ機能を発揮することができる。なお鍵暗号鍵を子局で生成する場合には、生成した鍵暗号鍵を親局に伝送する際には、子局毎あるいはすべての子局に共通な公開鍵を親局から通知を受けた公開鍵を使って暗号化すればよい。図16は、この発明に係わるポイントツーポイント型ネットワークのアーキテクチャの一実施の形態を示す図である。図16において、611～616はノード局であり、これらはループ状に構成され、そして、ノード局間の通信には無線もしくは有線回線が用いられる。当然ながら、本発明の実施されるネットワークのノード局の構成はループ状に限定されるものではなく、メッシュ状の構成等、他の様々な構成にも適用可能である。また、各々のノード局には、加入者網621～626が、有線回線もしくは無線回線を用いて接続される。

【0032】各々のノード局は、隣接するノード局から送信されるデータを受信して、当該データが本ノード局と接続する加入者網宛のデータであればこれを加入者網宛に送出し、そうでなければ他方に隣接するノード局宛に当該データを送出する。また、本ノード局と接続する加入者網より送信されるデータを、隣接するいずれか一方のノード局宛に送出する。図17は、図16に示した、無線回線を介して構成されるポイントツーポイント型ネットワークがATMを用いて通信を行う場合の、ノード局間のプロトコルスタックを示す。ポイントツーポ

イント型ネットワークにおいても、第三者によるデータの盗聴を防ぐために、ノード局のATM層に、セキュリティ機能を搭載する(ATM+Sec層)。ATM+Sec層にて行う、暗号化、復号の手順は、図3～図5に示す手順と同様に行うことができる。ATMセルの配送時に行う暗号化処理、復号処理の際に用いる共通鍵a、鍵aの配送時に行う暗号化処理、復号処理の際に用いる共通鍵b、鍵bの配送時に行う暗号化処理、復号処理の際に用いる公開鍵、秘密鍵を用いた場合の機能ブロック図を、図18に示す。ノード局間にて暗号化処理、復号処理を伴うATMセルの送受信を行う場合、まず、いずれのノード局にて鍵a、鍵bを生成するかを取り決める必要がある。図18の場合、ノード局aにおいて、これらの共通鍵の生成を行い、ノード局bとのATMセルの送受信を行っている。共通鍵の生成を行うノード局の定め方としては、例えば、ネットワーク構築時に共通鍵を生成するノード局を陽に定めておき、当該ノード局に対してのみ、共通鍵を生成し、送信する機能を搭載させる方法、また、全てのノード局内に共通鍵を生成し、送信する機能を搭載させ、ATMサービスの開始時に、いずれのノード局にて共通鍵を生成するかを、シグナリング等を用いて規定する方法、等が考えられる。

【0033】そして、ノード局a内の暗号化/復号化部21、ノード局b内の暗号化/復号化部22において用いられる鍵aは、ノード局a内の鍵a生成部23にて定期的に生成し、ノード局b宛に送信される。また、鍵aを送信する際に、ノード局a内にて暗号化処理を行う暗号化部24、ノード局b内にて復号処理を行う復号化部25において用いられる鍵bは、ノード局a内の鍵b生成部26にて定期的に生成し、ノード局b宛に送信される。この時、ノード局a内の暗号化部27にて鍵bの暗号化に用いる鍵は公開鍵であり、ノード局b内の復号化部28にて鍵bの復号に用いる鍵は秘密鍵である。ノード局aとノード局bとにおいて、暗号鍵の更新を行う場合、更新前の暗号鍵と更新後の暗号鍵とのいずれの鍵により暗号化処理、復号処理を行うかを、親局と子局との間に同期を取る必要がある。そのための一つの方法として、前出した加入者無線アクセスシステムにおいて示した、OAMセルを用いて行う方法を挙げることができる。その際の手順は、図11、図12と同様に行われる。ところで、前出した加入者無線アクセスシステムにおいて示した、暗号鍵の更新の同期を取る方法の一つである、GFCフィールドを用いる方法は、図16に示すノード局間にてATMセルの送受信を行う場合には適用できない。これは、本ノード局間のインターフェースとしては、UNIではなくNNI(ネットワークノードインターフェース)が用いられるためである。図19に、ノード局間で伝送される、NNIにて定義されるATMセルのフォーマットを示すが、NNIにて定義されるATMセルでは、ヘッダ31内にGFCフィールドが存在しな

いことが原因である。

【0034】そこで本発明では、NNIにて定義されるATMセルのヘッダ内の情報を用いて暗号鍵の更新の同期を取るため、VPIフィールド(12ビット長)もしくはVCIフィールド(16ビット長)のいずれか、もしくは両フィールドのうちの一部フィールドを、暗号鍵の更新の同期を取るために用いる方法を示す。そのためには、VPI値、VCI値のいずれか、もしくは両値を圧縮して運用する必要がある。図20に、VPI値圧縮の手順を示す。図20の例では、VPI値のみを圧縮して、VCI値については圧縮を行わない方法を示すが、当然ながら、VCI値のみを圧縮する方法、VPI値、VCI値の両値を圧縮する方法も、同様の手順にて実現できる。図20では、あるキャリアが提供するキャリア網71(例えば、図16に示すポイントツーポイント型ネットワーク)内において、ローカルなVPI値「VPI-L」を定義する。VPI-L値は、図20では11ビット長としているが、それ以下のビット長であっても良い。そして、キャリア網71のインターフェース部72、73では、外部より受信したATMセル内のVPI値をVPI-L値に変換してキャリア網内へ送信し、またキャリア網より受信したATMセル内のVPI-L値を当初のVPI値に変換して外部へ送信する。図20の場合、インターフェース部72において、外部からのATMセルの受信を、インターフェース部73において、外部へのATMセルの送信を行っている。

【0035】12ビット長にて定義されるVPI値と、キャリア網71内でローカルに定義されるVPI-L値との対応表721、731は、インターフェース部72、73内にて各自保持される。これらの対応表は、新たな仮想コネクションの設定要求時に、当該仮想コネクションのVPI値に、本VPI値に対応させる、キャリア網71内にて生成したVPI-L値とが、新たなエントリとして挿入され、仮想コネクションの解放時に、当該仮想コネクションのVPI値と、本VPI値に対応するVPI-L値とが記載されたエントリが、消去される。図20に示したVPI圧縮により、キャリア網71においてはVPIフィールド内に、11ビット長のVPI-L値が挿入されるため、図21に示すように、VPIフィールドの1ビット領域が未使用となる。そこで、この未使用となる1ビット領域(以後、本領域を空きビット領域と呼ぶ)を、暗号鍵の更新の同期を取るために用いる。なお、図21にて示したATMセルフォーマットは、キャリア網71内にてローカルに使用され、キャリア網71内のノードでは、VPIフィールド内の11ビット領域にてVPI値(VPI-L値)を認識し、残りの1ビットを、暗号鍵の更新の同期を取るためのビットと認識する。

【0036】図20では、キャリア網内でのVPI値の圧縮(VPI-L値への変換)を、インターフェース部内

に対応表を用意することにより実現する方法を示したが、他にも、例えば、MH(Modified Huffman)符号化方式のような圧縮アルゴリズム、そして当該アルゴリズムにて圧縮されたデータを復号するアルゴリズムをインターフェース部内に搭載することにより、VPIフィールド内に未使用ビット領域を生成し、これを暗号鍵の更新の同期を取るために用いる方法も考えられる。上記空きビット領域を、暗号鍵の更新の同期を取るために使用する例を、図22、図23に示す。なお、図22では、共通鍵の生成を行うノード局aよりノード局b宛にATMセルを送信する場合を、図23では、ノード局bよりノード局a宛にATMセルを送信する場合を示す。図22、図23共に、送信側では、ATMセルの暗号化に用いた暗号鍵を更新する度に、当該ATMセル内の上記空きビット領域1ビットを反転させて送信する。そして受信側では、受信したATMセルの当該領域1ビットが、前回受信したATMセルの1ビットと反転した値であれば、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたATMセルであることが分かるため、以後、当該領域の前記1ビットが反転したATMセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。

【0037】なお、前述のシェアードメディア形アクセスネットワークでは、GFCフィールド内の特定の1ビットを鍵更新の同期用に割り当てるとしていたが、本実施例と同様にVPI/VCIを圧縮して、空きビット領域を同期用に割り当ても良いことは付言するまでもない。また、本実施の形態では、VPI値、もしくはVCI値を圧縮することにより生じる空きビット領域を、暗号鍵の更新の同期を取るために使用しているが、その他にも、キャリア網内に閉じたローカルな制御を提供するために、本領域を使用することが可能である。ATMセルのヘッダ内には、当該ATMセルの損失の優先表示を行うCLP(Cell Loss Priority)ビットが1ビットのみ用意され、本値を元に、ネットワーク内ではATMセルの優先制御を行う。しかしながら、CLPビットにて表示可能な優先レベルは2レベルのみであり(CLP=0、CLP=1; CLP=0の方が優先度が高い)、より細かな優先レベルを表示することは不可能である。そこで、任意のネットワーク内において、よりきめ細かなATMセルの優先制御をローカルに実行するために、VPI値、もしくはVCI値を圧縮することにより生じる空きビット領域を、ATMセルの優先度表示に使用しても良い。ATMセルの優先度を、CLPビットと当該空きビット領域とを組み合わせて表示することにより、4レベルの優先レベルの表示が可能となり、CLPビットのみを用いた場合に比べてより細かな優先制御の実現が可能となる。

【0038】当該空きビット領域は、上述したような暗号鍵の更新の同期情報やセルの優先度といった情報の記

載に利用する他にも、例えば、より強固な誤り制御を提供するために、ATMセル内情報に対するパリティビットの設定に使用する等、様々な制御情報の記載に用いることができる。特に、ATM通信の標準化団体で規定されていない制御情報をネットワーク内にてローカルに規定してATMセル内に記載したい場合に、ATMセルヘッダの圧縮により当該空きビット領域を生成すれば、これが可能となる。

【0039】

10 【発明の効果】以上説明したように、本発明は、親局と子局との間でのシェアードメディアを介したポイントツーマルチポイント通信を提供する上でのセキュリティ機能、そして、ネットワーク内のノード局間でのポイントツーポイント通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ATM層において、ATMセルに対して暗号化処理を施して当該ATMセルを送信するというセキュリティ機能を新たに提供することで、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ATMセルの送信時の暗号化処理、復号処理の際に用いる共通鍵(セル暗号化鍵)、そしてこの共通鍵の送信時の暗号化処理、復号処理の際に用いる共通鍵(鍵暗号化鍵)の更新に伴う、親局と子局との間で使用する鍵の更新の同期を、GFCフィールドもしくはOAMセルを用いて陽に取ることで、そしてネットワーク内のノード局間で使用する鍵の更新の同期を、VPIフィールドまたはVCIフィールドを圧縮することにより生じる空きビット領域、もしくはOAMセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

30 【0040】また、ATMセルヘッダを圧縮して、VPIフィールド、VCIフィールドとはじめとするATMセルヘッダ内に、ATM通信の標準化団体で規定されていない、ネットワーク内にてローカルに定義した制御情報を記載するための領域を確保することにより、新たな制御セルを挿入することなく、これらの制御情報の通知が可能となるため、制御セルの挿入に伴うスループットの低下を防いだ上で、より高度なネットワーク制御の実現が可能となる。

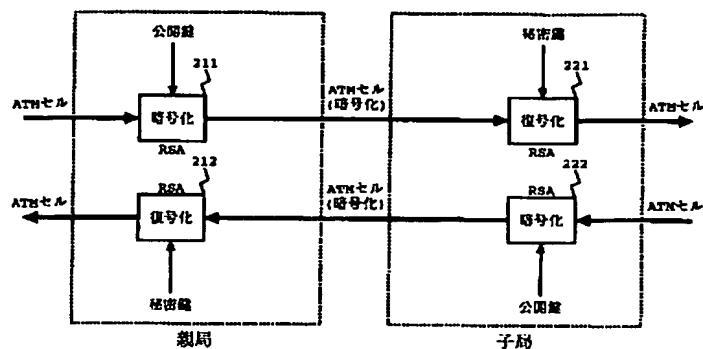
【図面の簡単な説明】

【図1】この発明に係わるシェアードメディア型ネットワークの一つ、加入者無線アクセスシステムのアーキテクチャの一実施の形態を示す図。

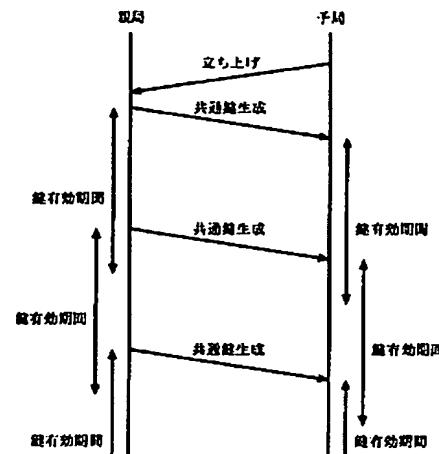
【図2】図1に示した加入者無線アクセスシステムがATMを用いて通信を行う場合のプロトコルスタックを示す図。

50 【図3】図1に示した加入者無線アクセスシステムがA

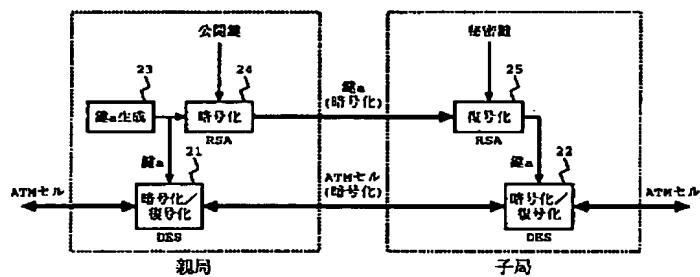
【図4】



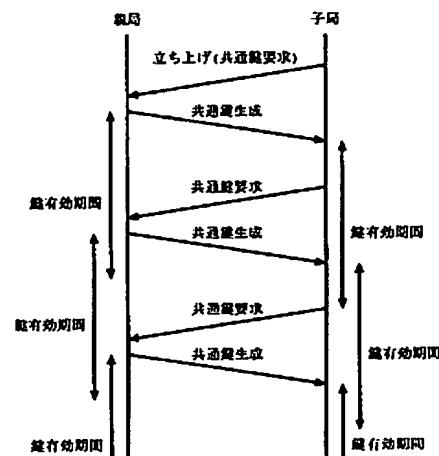
【図7】



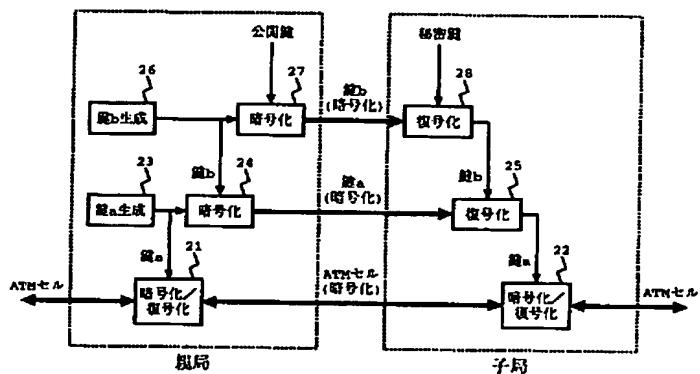
【図5】



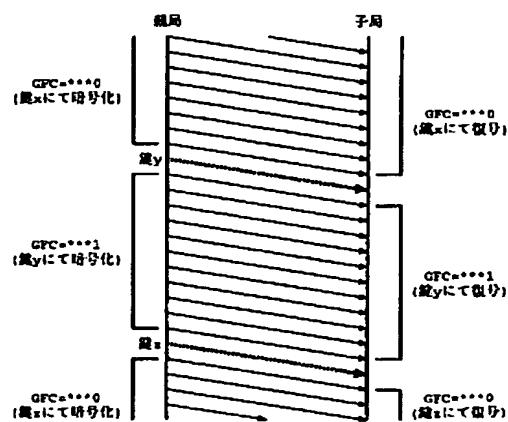
【図8】



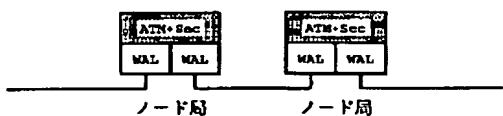
【図6】



【図10】

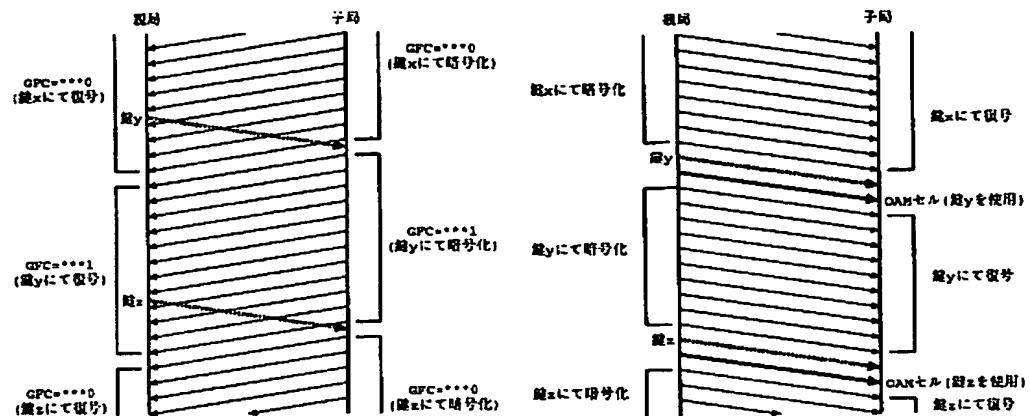


【図18】

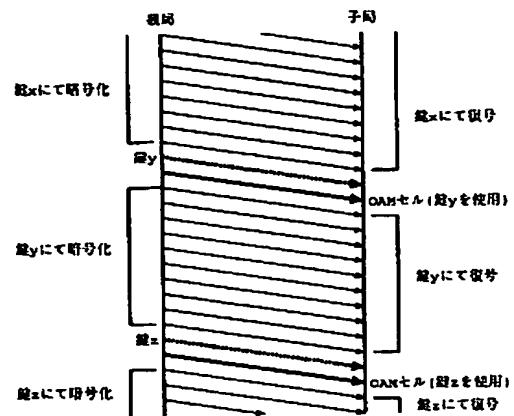


BEST AVAILABLE COPY

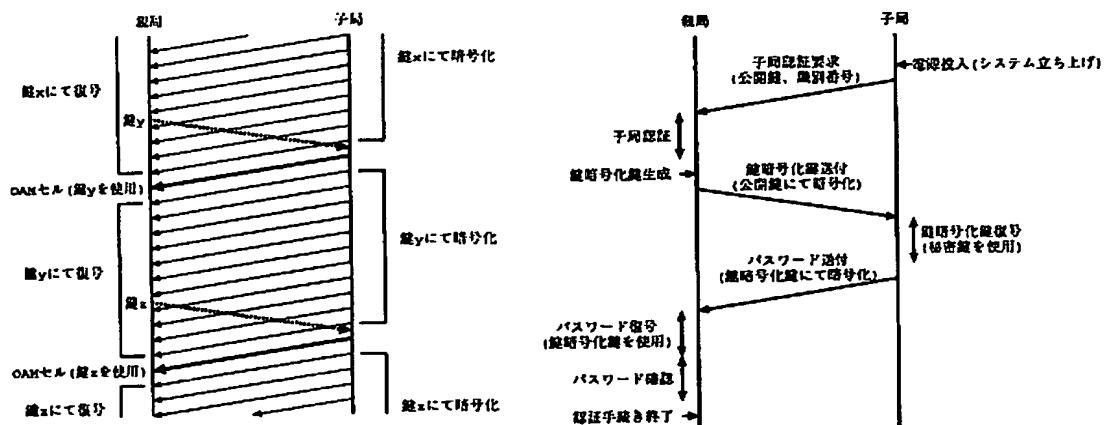
【図11】



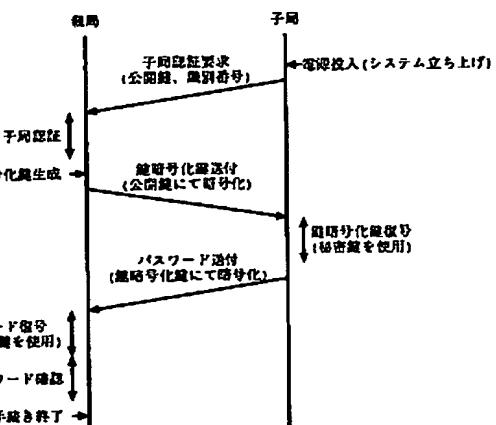
【図12】



【図13】

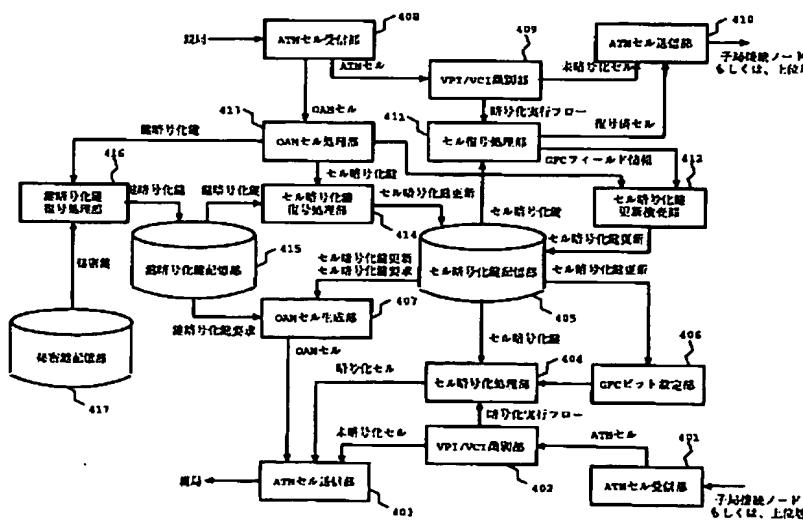


【図14】

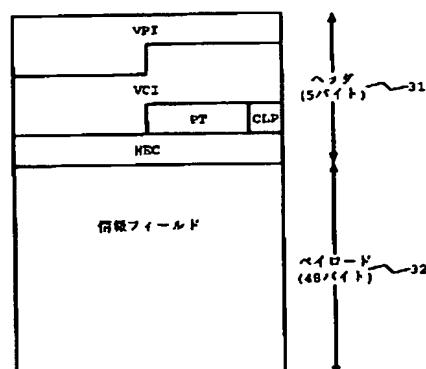


BEST AVAILABLE COPY

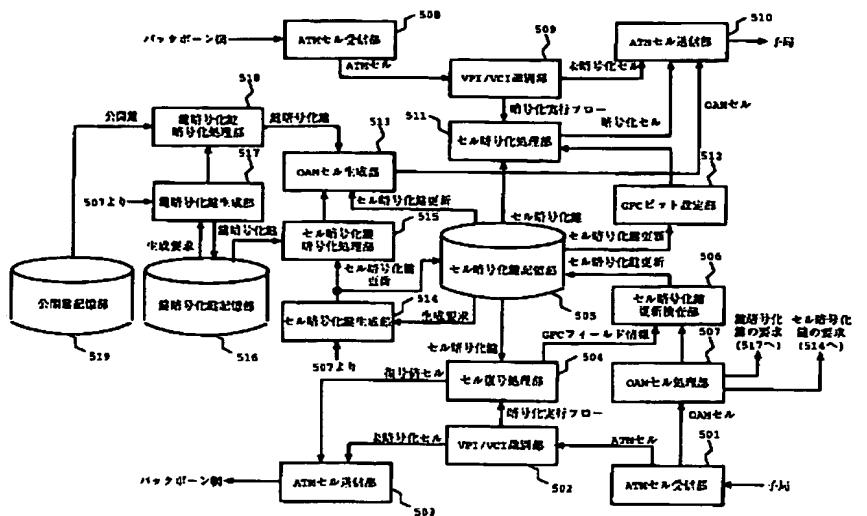
【図15】



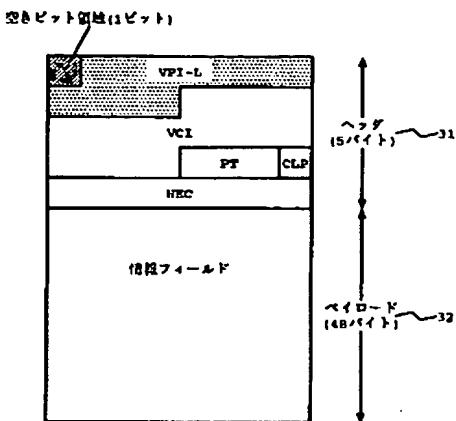
【図20】



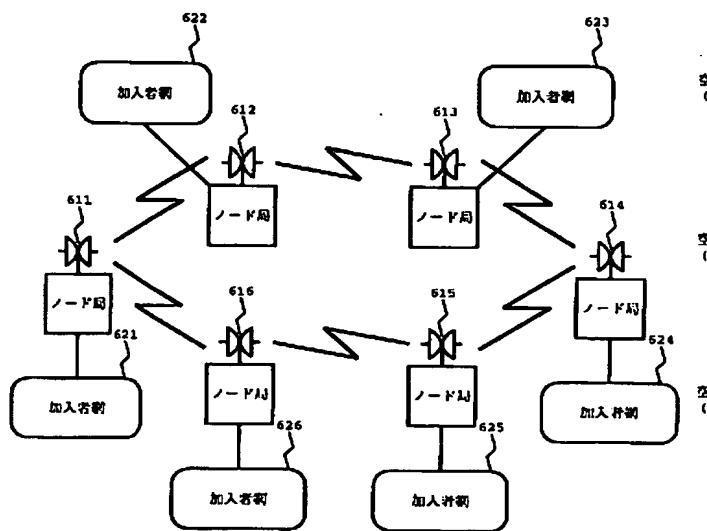
〔図16〕



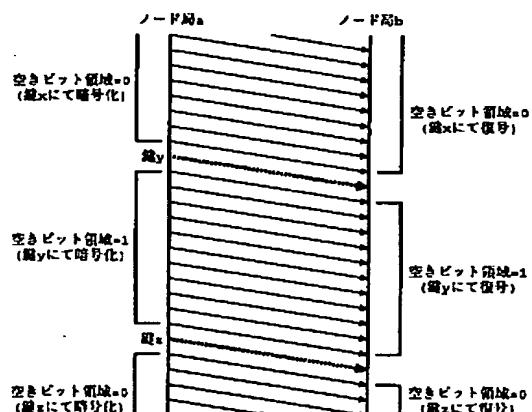
〔図22〕



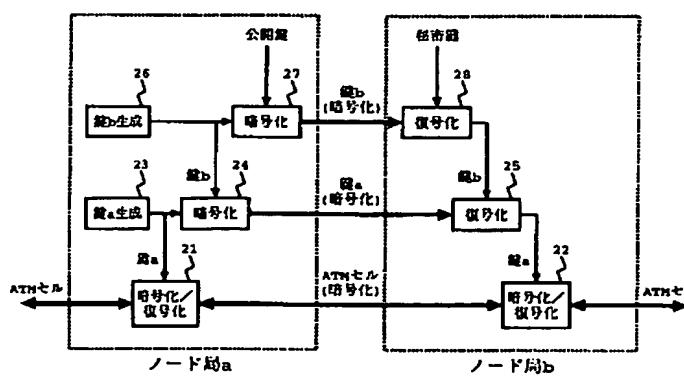
[図 17]



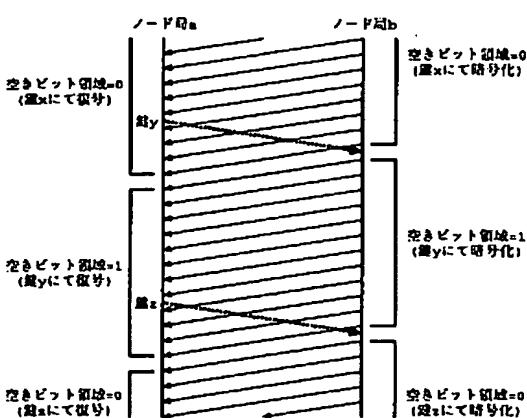
[图 23]



[図 19]

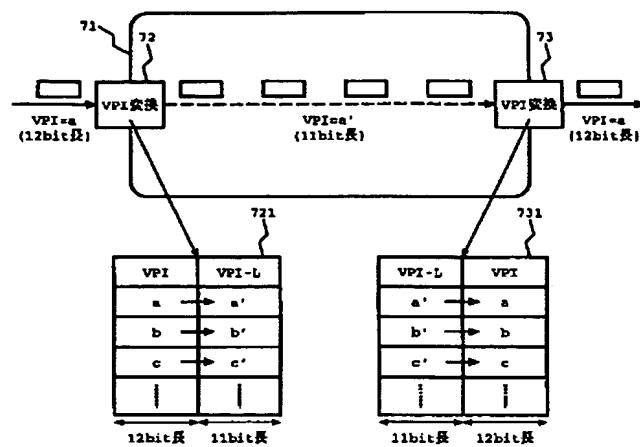


[図24]



BEST AVAILABLE COPY

【図21】



フロントページの続き

(72)発明者 角田 啓治

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

F ターム(参考) 5J104 AA01 AA16 AA34 EA17 EA19
JA13 JA28 JA31 NA02 PA01
5K030 GA15 HA10 HB11 HB29 HC14
JL01 JT09 LD19
9A001 CC02 CC05 CC08 EE03 EE04
HH15 JJ12 KK56 LL03